CLARKSVILLE MONTGOMERY COUNTY SCHOOL SYSTEM

Department: Technology
Policy Number: TCH-A002
Effective Date: 7/18/11

ADMINISTRATIVE POLICY

The online version of this policy is official. Therefore, all printed versions of this document are unofficial copies.

TECHNOLOGY ACCEPTABLE USAGE

Clarksville-Montgomery County School System (CMCSS) has developed an extensive technology infrastructure, including hardware, software and connectivity equipment toward the purpose of improving the District's educational, administrative and clerical functions. The significant ongoing investment in technology is in part justified by two promises:

To better prepare students for life and work in a future filled with technology laden changes, and use.

To increase the productivity of current and future staff.

This investment must be protected from potential misuse and deliberate abuse. CMCSS uses a Children's Internet Protection Act (CIPA) compliant solution to prevent student access to materials the district deems harmful and to block internet access to inappropriate sites, including child pornography and obscenity. This policy clarifies roles and responsibilities in the use of CMCSS technology, both hardware and software, to preserve the integrity and usability of these resources to benefit and serve all clients. Failure to comply with this policy may result in the suspension of privileges, internal investigation, and/or criminal prosecution. CMCSS must be strict in these matters, not only because of the value of the resources, but also to ensure a safe and productive learning and working environment for our students, faculty, and staff. These rules apply to all CMCSS computing resources.

The intent of this policy is to raise awareness about what is appropriate, ethical, legal and professional use of a valuable shared resource, not to enumerate all uses that are or are not appropriate.

Acceptable use of CMCSS information technology resources is based on common sense, common decency, and civility applied to the networked computing environment. There is no expectation of privacy by users when using the internet or electronic communications. The district reserves the right to monitor, inspect, copy, review and store (at any time and without any prior notice) all usage of district computers, computer systems, and electronic communications. The district may access district-owned or networked computers for maintenance, upgrades, and at any time of suspected abuse of district policy. Appropriate use of these resources must be consistent with the purpose for which the computer/security accounts (log-ins) were originally requested and provided. Privately owned devices connected to CMCSS network, whether wired or wireless, are subject to monitoring, inspection, possible confiscation, and investigation. Attaching privately owned devices to CMCSS network is a privilege and is subject to all provisions within the Technology Acceptable Usage Policy.

Expressly prohibited are any uses:

Which benefit any political, religious, or commercial organization.

Which are illegal, obscene, or for profit.

That adversely affect the reputation or image of CMCSS.

Of unauthorized attempts to log in to any network as a system administrator. This could result in cancellation of user privileges.

Of unauthorized disclosure of personal information.

Involving vandalism. Vandalism is defined as any malicious attempt to harm or destroy CMCSS data, data of another user, or other CMCSS computing facilities or equipment. This could result in cancellation of privileges.

Network Security

Network passwords and account information are only given to authorized personnel.

Only users with valid CMCSS network accounts are authorized to use the CMCSS network and computer equipment. Employees and students must only use their assigned network account.

All computer users must always secure their computer(s) and network log-in before leaving their room or office. Do not allow anyone to use your computer (with the exception of a CMCSS Technology Department employee). The individual assigned a computer/security account is accountable for any and all transactions entered under that computer/security account login.

For the protection and security of the CMCSS data, all equipment attached to the CMCSS physical network (equipment located at a CMCSS facility either wired or wireless) must be CMCSS property or have received approval from the IT Department management.

Use of software designed to gain passwords or access beyond the rights assigned to a user or computer is strictly prohibited. Use of such programs risk the security of the network and is considered “hacking”. The intent to obtain unauthorized access is a violation of State and Federal law. Violators will be prosecuted. Should you inadvertently discover passwords or any other method used to control unauthorized access; this must be reported immediately to supervisory personnel in the room (in case of students) or the Chief Technology Officer (in case of staff).

The following activities and uses of the CMCSS network are prohibited:

1. Downloading, installation or use of programs that infiltrate computing systems and/or damage software components, including “viruses” and “worms”.

2. Downloading, installation or use of any program or software not listed on CMCSS software approval list is prohibited without prior written authorization of IT Department management. Updates of existing IT installed software are permitted.

3. Intentionally disrupting network traffic, crashing the network, or gaining unauthorized access to the files of another user.

4. Use of the network to personally attack, harass, threaten, or bully another person intentionally or recklessly publish false information about another person.

5. Use of inappropriate language in any type of communication, including, but not limited to, language that is illegal, vulgar, profane, abusive or threatening.

6. Any access to the network through false identity including anonymous communication, falsifying, concealing, or misrepresenting the user’s identity or sharing or loaning network accounts.

7. Mass e-mailing of unsolicited and unwanted messages ("spamming"), including text, software, video images, graphics and chain letters.

8. Downloading music and sound recording for non-instructional purposes without the permission of supervisory personnel.

Workstation/Computer Use

All employees and students are prohibited from installing any software on any computer unless authorized in writing by the IT Department management. Illegal download or use of copyrighted software, music, videos, pictures or other files is strictly prohibited.

All employees and students are prohibited from using any computer for illegal or commercial activity.

Any desktop application designed to limit access to students or staff, other than those used by the IT Department for network security purposes, is prohibited.

Changing or tampering with any computer's vital system configuration is strictly prohibited.

Any action which violates Board or Administrative policies, local, state or federal law is prohibited.

Computers found to be tampered with or computers with unapproved software or files will be re-formatted and restored to compliance.

All loaned computer equipment loans must comply with the district Equipment Loan Agreement (BUS-F012).

Internet Connectivity

CMCSS provides internet connectivity to improve the District's educational, administrative and clerical functions. Responsible and ethical use of the wired and wireless network system is required. Internet use is intended for valid and legitimate district related purposes. Classroom use of the internet is intended for instructional related purposes only. Internet connectivity may not be used for personal gain or political or religious views or in any illegal, offensive or unethical manner. All internet traffic is subject to review at any time by authorized CMCSS personnel. In the event of a violation of this policy, the device used in such violation (either private or property of the CMCSS) may be confiscated and searched. There is no expectation of privacy.

It is the responsibility of all members of the CMCSS staff to supervise and monitor usage of the online computer network and access to the internet in accordance with this policy and the CIPA.

Viruses and Virus Protection

The CMCSS IT Department will provide all virus protection and related software for all CMCSS workstations and servers. Virus protection and related software will be installed by authorized IT personnel unless otherwise approved by the IT Department.

Do not open any e-mail attachments from anyone you do not know. Never send anyone e-mail you suspect may contain a virus. The intentional spreading of messages or files containing damaging or destructive programs or data is against federal law. Violators will

be prosecuted. If you suspect your computer may contain a virus, contact the IT Department immediately.

There are many virus hoaxes. Never delete system files from a computer in order to remove a potential virus without first checking with the IT Department to ensure the virus is valid and not a hoax.

Copyright Policy

All students and employees will comply with all applicable copyright laws in the use of all media and materials and model legal and ethical practices related to technology.

E-mail

The CMCSS e-mail system has been provided for the internal and external communication of employees and board members. Responsible and ethical use of the e-mail system is required. The e-mail system may not be used for personal gain or political or religious views or in any illegal, offensive or unethical manner. Personal e-mails should be limited. All e-mail is the property of CMCSS and, as such, is subject to review at any time by authorized CMCSS personnel.

Cell Phones

This policy is meant to ensure the safe operation of both company vehicles and private vehicles while an employee is conducting business on work time. The use of a cell phone while driving may present a hazard to the driver, other employees and the general public.

CMCSS employees are not permitted to use cell phones for voice communications, e-mail communications, or text communications while operating a CMCSS motor vehicle (Ref. OPS-A006).

In addition, employees must adhere to all local, state or federal rules, regulations, laws or other ordinances regarding the use of cell phones while driving personal vehicles. Employees should check with local authorities if they are unsure whether the use of a cell phone while driving is prohibited in a particular area. It is recommended that employees not use hand held cell phones for business purposes while driving personal vehicles. Employees may use hands-free cell phones to make business calls in accordance with the law.

Additionally, personal telephone calls should be limited both in time and nature so as not to interfere with work responsibilities. If an employee abuses this privilege while using a CMCSS-issued cell phone, the employee will be responsible for reimbursement to the school system.

Server Software

Only authorized IT Department personnel will install software to servers.

When a suspected violation of the above agreement becomes known, the incident should be reported to the appropriate supervisor and the Chief Technology Officer. If the incident is in violation of Board or Administrative Policies, the supervisor shall take appropriate action. In order to prevent further possible inappropriate activity, the user's computer/security account access may be temporarily blocked. If this is deemed necessary, every effort will be made to inform the user prior to this action and to re-establish the connection as soon as deemed appropriate. Any determination of

inappropriate use, serious enough to require disconnection, should also be promptly communicated to the user's supervisor.

Technology Abuse

In the event a CMCSS employee becomes aware of the misuse or abuse of CMCSS technology, he or she should act in accordance with the district's Computer Abuse Discovery Procedure (TCH-P026).

Associated Documents: Internet Usage Agreement (TCH-F018)
Equipment Loan Agreement (BUS-F012)
Computer Abuse Discovery Procedure (TCH-P026)
Children's Internet Protection Act
User Password Policy (TCH-A003)
Use of Cell Phone While Operating CMCSS Vehicles (OPS-A006)
Employee Handbook (HUM-M001)

Revision History:

Date:	Rev.	Description of Revision:
4//17/06		Initial Release
6/30/08	A	Add "computer systems, and electronic communications" to fourth paragraph, third sentence.
9/17/08	B	Second sentence in second paragraph added to comply with TN Senate Bill No. 3702, obscene added to second sentence under Expressly prohibited are any uses, add associated documents
10/23/08	C	Add fifth sentence under Expressly prohibited are any uses, add second paragraph under Internet Connectivity and add Children's Internet Protection Act to Associated Documents.
07/08/09	D	Add Computer Abuse Discovery Procedure reference.
12/10/09	E	Change form number in associated documents from TCH-F021 to BUS-F012.
09/27/10	F	Added last sentence to "Internet Connectivity" section.
7/18/11	G	Added Children's Internet Protection Act to second paragraph. Inserted "value of the resources" in place of "real value of the facilities" in second paragraph. Changed wording of last sentence in second paragraph. Added last two sentences in fourth paragraph. Deleted "will result in cancellation of privileges" from first paragraph on page 3. Inserted "could result in cancellation of privileges". Under Network Security, changed 2nd paragraph. Miscellaneous grammatical changes. In #2 under prohibited network activities, added "not listed on CMCSS software approval list is prohibited". Added reference to BUS-F012 in Workstation/Computer Use. Internet Connectivity – added "wired and wireless network" in second sentence. Cell Phones – Changed third paragraph.
3/5/12	H	Updated Cell Phone section to reflect the attached information, added OPS-A006 and HUM-M001 to Associated Docs.

*****End of Policy*****